SUCSES:
Survivability Using Controlled SECurity Services

Gene Tsudik
UC Irvine

Dan Boneh
Stanford University

http://sconce.ics.uci.edu/sucses

Administration

- Start date: Sep. 1999
  Duration: 36 months

- Agent: AFRL, Bob Kaminski.

- Parties involved:
  USC/ISI
  UC Irvine: Gene Tsudik
  Stanford: Dan Boneh

- No clearance.

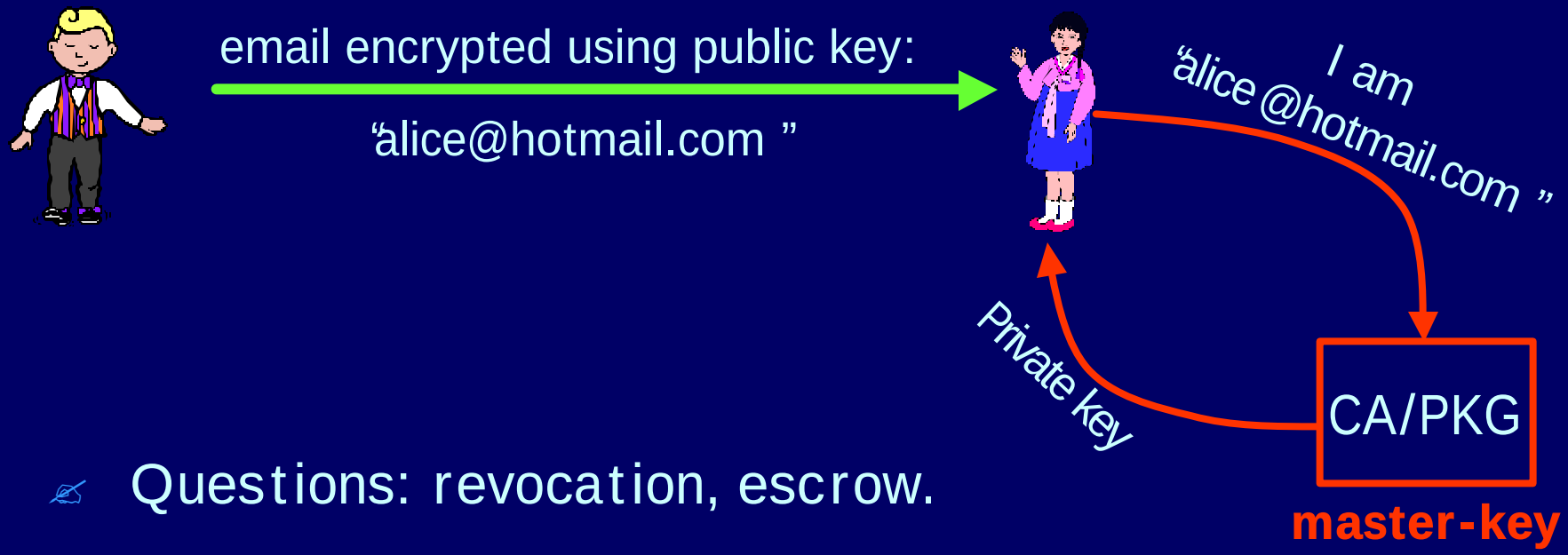
Status: Started 09/99

- SAS - Server Assisted Signatures.
  - Off-loaded signatures: server does most work, client only does hashing. Ideal for low power handhelds.
  - Software available for download. Eudora plug-in support.
- SAG - Server aided RSA key gen, Server aided RSA sigs.
  - PalmPilot prototype software available for download.
- mRSA - Mediated decryption and signatures.
  - Provides easy revocation of security capabilities.
  - Software libraries ready. Eudora plug-in support.
- IBE – Identity Based Encryption. Initial deployment.
  - Optimized library implementing IBE cryptosystem available.
  - Backend CA/PKG system running at Stanford.
  - Support for Outlook, Hotmail, pine, mail-proxy all available.

Identity Based Encryption/PKI

Identity Based Encryption (IBE)

- IBE: Public key encryption scheme where public key is an arbitrary string (ID).
  - Examples: user's e-mail address, current-date, …



- Questions: revocation, escrow.

IBE System

- IBE system is made up of 4 algorithms:

  setup: generate sys-params and master-key.

  keygen: given pub-key ID and master-key output priv-key.

  Encrypt: using pub-key ID (and sys-params)

  Decrypt: using priv-key.

- Main use of IBE:
  - reduce need for online pub-key or cert directory.

History

- 1984: IBE suggested by Shamir.
  - RSA: cannot map name to pub key = (N,e).
  - ElGamal: pub-key = g^x (mod p). CA cannot get x.
  - Until now, no satisfactory solution.
- Boneh-Franklin (Crypto 2001): (thanks to DARPA)
  - First practical IBE cryptosystem.
    based on Weil pairing from algebraic geometry.
- Performance (1024-bit security, 1GhZ P3):
  - Keygen time: 3 ms.
  - Enc/dec time: 90 ms. Open source library.

Application 1: simple secure Email

- Bob encrypts mail with pub-key = "alice@hotmail"
  - Easy to use: no need for Bob to lookup Alice's cert.
  - Bob can send mail to Alice even if Alice has no cert.

- Bob enc with pub-key = "alice@hotmail || current-year"
  - Key expiration:
    Alice's private key in effect for one year only.

- Bob enc with pub-key = "alice@hotmail || current-date"
  - Short lived private keys: revocation + mobility.
  - Bob can send mail to be read at future date.

SCRIBE: ID based secure e-mail

- Current deployment: http://identicrypt.stanford.edu
  - Backend CA/PKG system running at Stanford.
    - User mgmt and authentication, logging, key-gen.
  - Plug-ins for Outlook, hotmail, pine, and mail-proxy.
    - Key manager runs on user's machine. Normally hidden.
  - Emphasis on ease of use and ease of installation.
    - Fully transparent to sender: promotes use of secure mail.
- Ephemeral public-keys: one week lifetime
  - Pub-key: purpose=email&version=1.0&email=dabo@cs&date=31
  - Plug-in downloads new priv. keys from PKG as needed.
- User identification:
  - use SSH model: first time weak, then strong(er).

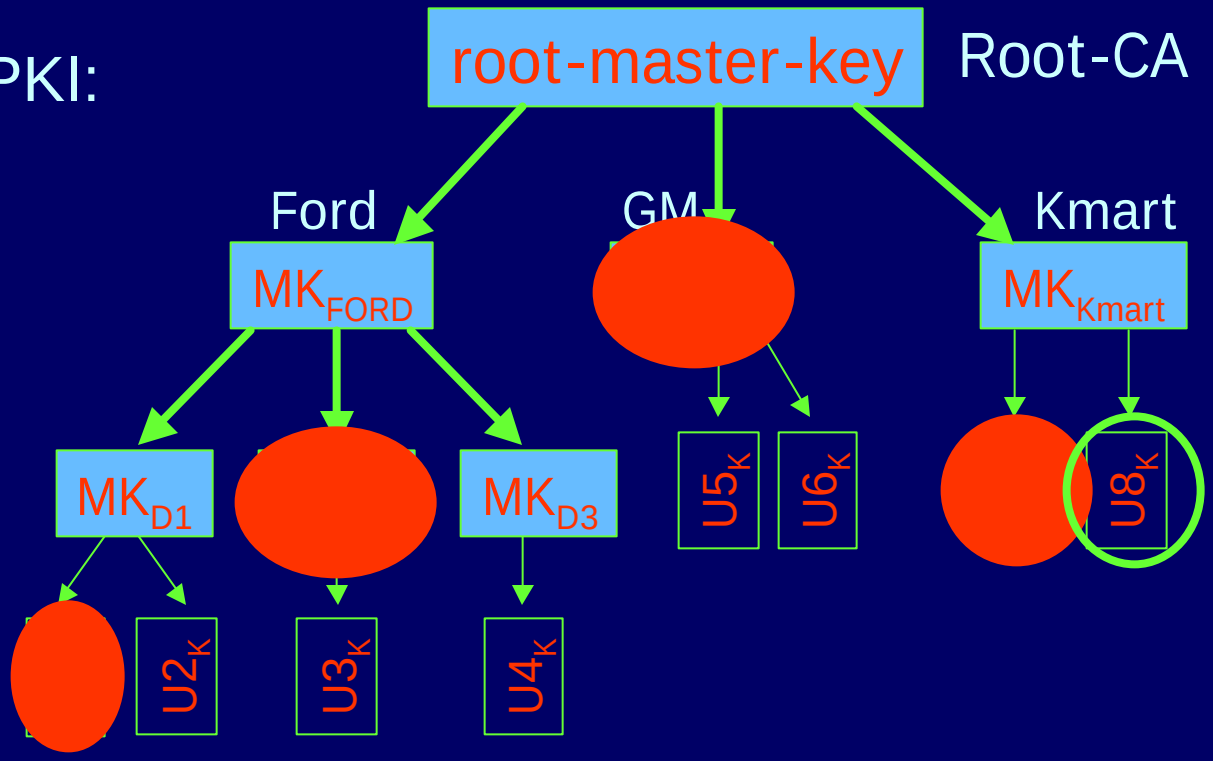
Future work (SCRIBE)

- Enable users to upgrade to RSA keys:
  - Alice and Bob exchange secure e-mail using IBE.
  - At any time: exchange RSA public keys using authenticated IBE.
  - Benefit: disable key escrow by PKG.
  - Downside: public keys are no longer ephemeral.
    - Harder to achieve mobility and revocation.

- Manage CA/PKG master-key on IBM 4758.
  - Implement IBE cryptosystem on 4758 card.
  - Support key sharing and backup of IBE root key.

ID based PKI: IBE Hierarchy (BHL 02)

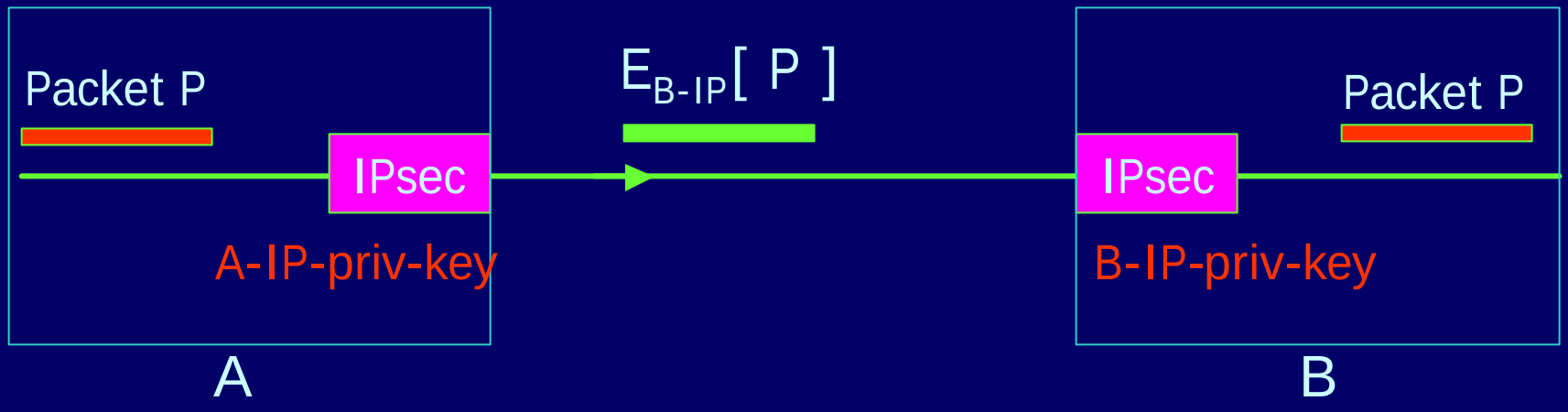
- ID based PKI:



- Security: No coalition of entities can get a user key not under their control.
- BHL-02: two levels with limited collusion resistance.

ID based stateless IPsec (A02)

- Stateless IPsec: (no IKE)
  - Site A encrypts packet to site B using B's IP address as public key.



- Implemented on top of Linux.
- Planned implementation using SEM architecture.

Other applications for IBE

- Simple certified e-mail:
  - Sender encrypts e-mail using

    std. || sender-email || subject-line || mail ID.
  - To read e-mail, receiver requests key from PKG.
  - PKG sends signed receipt to sender.
- Ephemeral keys on handhelds:
  - Handheld loss does not lead to loss of long term key.
- ID based stateless IPsec:
  - Implemented on top of Linux. Planned SEM Support.
- Fast-track SSL session establishment. [BS02]

Bonus: Short signatures (BLS 01)

- Short digital signatures needed when:
  - Signature is typed in by a human.
  - Very low bandwidth, e.g. on a postage stamp.
- Recommended sizes for existing signatures:
  - RSA: 1024-bits (using 1024-bit modulus).
  - DSA: 320-bits
- New signature scheme based on Weil pairing:
  - sig-size = 160-bits,
  - Same security as 320-bit DSA.
  - Signing: 4ms (3xRSA), verify: 140ms. (1GhZ, P3)

mRSA – Mediated RSA

mRSA/SAS New Features Update

- ID-mRSA: simple, online, identity-based variation of mRSA
  - Fine-grained revocation
  - Performance same as mRSA (approx. 4xRSA)
  - Only site-specific certificates (modified X.509v3)
  - Eudora plug-in available for encrypted email
- Forward Security: protection against key compromise; both (or one) SEM and user "evolve" key shares periodically.
- Multi-SEM Support: high-availability + security.
  - Single PK per user
  - User can use any one of t SEMs
  - Mitigates compromise of a SEM
- Unified plug-in base (mRSA, SAS, id-MRSA)
  - Outlook version planned

Pointers:

SUCSES web page:	*sconce.ics.uci.edu/sucses*
IBE web page:	*crypto.stanford.edu/ibe* *identicrypt.stanford.edu*
SAG web page:	*crypto.stanford.edu/~dabo/palmrsa*